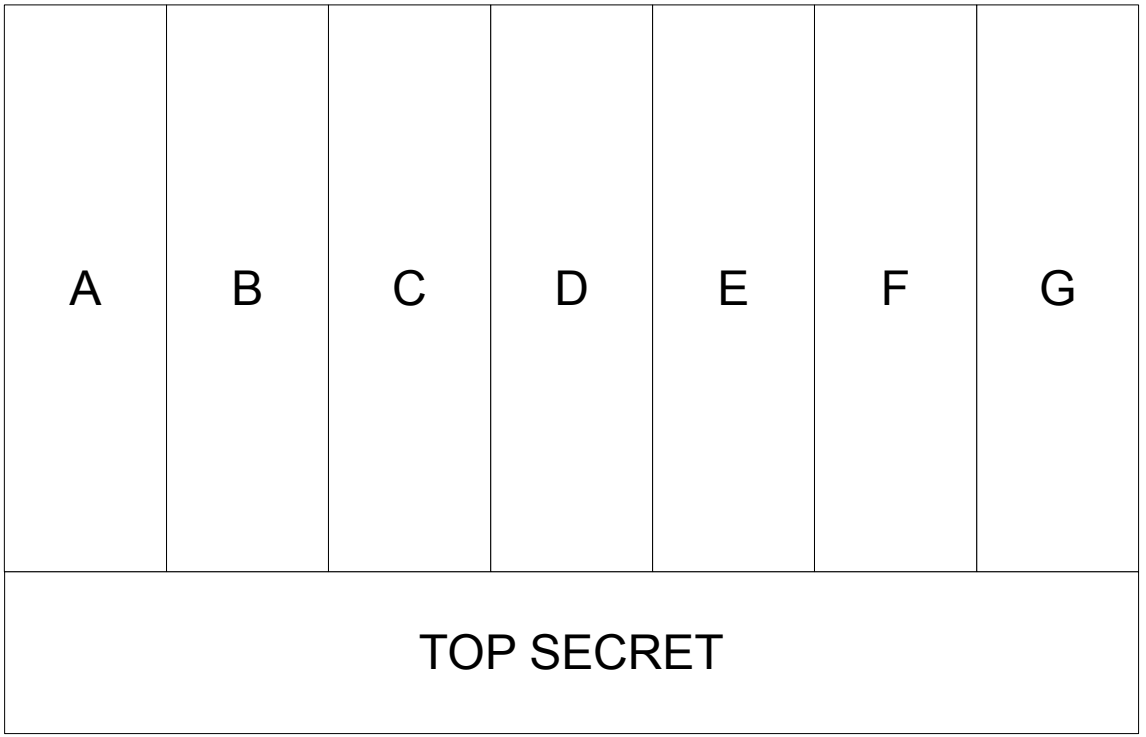
Multilateral Security

Recap: multilevel security

Multilateral security



Applications

- Military
- Medical systems
- Financial institutions
- Law firms

Compartmentation

- Military used codewords in addition to classification
- Person has access to document, if he is cleared for all the codewords
- Goal: more granular access control

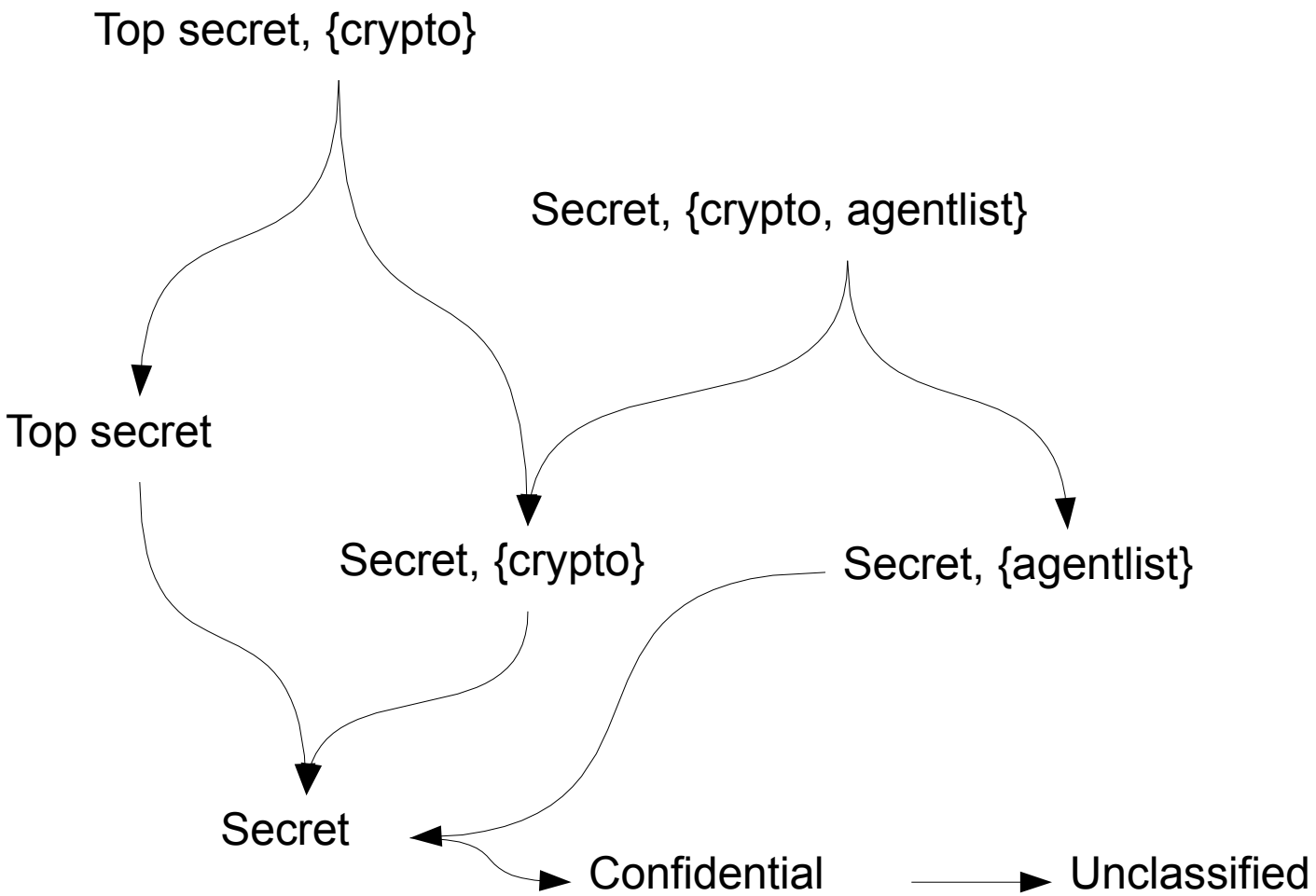
Problems with codewords

- Derived works contain all codewords from the sources
- Partial solution: clear top people for lot of codewords

The lattice model

- Variant of the Bell-LaPadua model
- Order relation: A > B, if person who can access A, can also access B
- Example:
  Secret, agentlist > Secret > Confidential

The lattice model (2)



Problem with the lattice model

- If there are enough compartments, it becomes impossible to share data
- Solution: create least upper bounds
  - Example: top secret classification can read secret files with all labels
- Frequent use: combine data from different compartments and downgrade after sanitization

The Chinese Wall

- Used in various professions to prevent conflicts of interest
- People who give investment consultations do not talk to exchange brokers
- Often the customers are competitors
  - Financial adice, law firms, advertising agencies
- Policy: different workers deal with different customers/areas

Medical information

- Main threat: social engineering
  - Attacker phones hospital asking for patient records
  - In one health authority, 30 calls per week
  - Applicable in other fields too
- It is important to limit amount of data visible to any person
  - Often doctors want to see max. amount of data

More problems

- Some bits can be inferred from other bits
  - Example: diseases can be inferred from prescriptions
- Electronic patient record – single record containing all the medical information about a patient

Security measures

- Archive old patient records
- Honey trap – bogus patient records with celebrity names
- Business rules – if employee looks at records, there must be an insurance claim later

The BMA model

- BMA = British Medical Association
- Goals
  - Enforce the principle of patient's consent
  - Prevent too many people from getting access to too large databases of identifiable records
  - Provide accountability
- Medical record = maximum set of facts relating to a patient and to which the same staff had access
  - Patient can have more than one record

The BMA policy

- Access control: each record is marked with ACL
  - People not in ACL cannot access record
- Record opening: clician may open a record with herself and the patient on the ACL
- Control: one of the clinicians on the ACL must be marked as being responsible
  - Only she may alter the ACL

The BMA policy (2)

- Consent and notification: the responsible clinician must notify patient:
  - All the changes to the ACL
  - When responsibility is transferred
  - Modifications require patient's consent
- Persistence: no one can delete clinical information
  - Unless the appropriate time has been passed

The BMA policy (3)

- Attribution: all accesses to record are logged
- Information flow: information derived from record A may be appended to record B iff B's ACL is contained in A's
- Aggregation control: there shall be effective measures to prevent the aggregation of personal health information
  - Patient must be notified, if person with wide access rights is added to their ACL

The BMA policy (3)

- Trusted computing base: computer systems must contain subsystem that enforces the above principles
  - This subsystem must be evaluated by independent experts

The security models

- All are mainly concerned with malicious insiders
  - Goal is to prevent one person from accessing too much data
- Lattice model isolates compartments, but prevents sharing
- Chinese wall is more centralized than the BMA